PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:	)
	)
Barton et al.	) Art Unit: 2137
	)
Application No. 09/916,600	) Examiner: Pyzocha, Michael J.
	)
Filed: 07/26/2001	) Atty. Docket No.
	) NAI1P020/01.139.01
For: SYSTEM, METHOD AND COMPUTER	)
PROGRAM PRODUCT FOR ANTI-VIRUS	) Date: 08/21/2008
SCANNING IN A STORAGE SUBSYSTEM	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

REPLY BRIEF (37 C.F.R. § 41.37)

This Reply Brief is being filed within two (2) months of the mailing of the Examiner's Answer mailed on 06/23/2008.

Following is an issue-by-issue reply to the Examiner's Answer.

Issue #1:

The Examiner has rejected Claim 42 under 35 U.S.C. 112, first paragraph, as providing new matter not originally described in the Specification.

Group #1: Claims 42 and 43

The Examiner has withdrawn the rejection under 35 U.S.C. 112, first paragraph.

Issue #2:

The Examiner has rejected Claims 1-2, 4-7, 10-18, 20-23 and 26-40 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent Publication No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700.

Group #1: Claims 1, 2, 4, 5, 10, 11, 15-17, 18, 20, 21, 26, 27, 31-34 and 39

With respect to Claim 1, the Examiner continues to rely on the following excerpt from Flint to meet appellant's claimed "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

> "The third activity waits for user input (block 421). When user input is received, it is evaluated to determine if the user has requested that a particular file be scanned (block 423). If so, an on-demand scan is performed using the requested file as the scan set as described below with reference to FIG. 6. **If the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed.** When the user has previously requested the scanning facility be stopped (as described next), the user can request it be restarted (block 431). Any other user input, including a request to stop the scanning facility, is processed at block 433. Such user input also includes changing preference parameters that control the overall functioning of the anti-virus software. The user can also specify which files to include in a pre-defined scan set that is used by the on-demand scan of FIG. 6. The handling of such user input is well understood in the art and is not

> discussed further. Moreover, it will be appreciated that the input interface is conventional and thus not illustrated." (Col. 9, lines 5-24 - emphasis added)

Appellant respectfully asserts that the above excerpt from Flint simply discloses "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed". Thus, Flint only teaches a user terminating the anti-virus program, and not "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module," as claimed by appellant.

To further clarify this distinction, appellant respectfully points out Fig. 8 in Flint, as referred to in the above excerpt. Specifically, Fig. 8 teaches writing to permanent storage (block 803) even after a user has specified to terminate the anti-virus program (block 429 of Fig. 4). Appellant respectfully asserts that this clearly *teaches away* from appellant's claim language since appellant specifically claims "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added). Allowing the data to be written to storage or read from storage without fully completing a scan, as in Flint, would provide the opportunity for malicious code to execute and/or proliferate on the systems sought to be protected. Appellant's claimed invention is clearly capable of avoiding such a situation.

In the Advisory Action dated 05/16/2005, the Examiner has argued that Makita, in combination with Flint, teaches appellant's claim language. Specifically, the Examiner has argued that Makita teaches "[t]he storage location retrieves the data and performs an internal virus check on the data before it sends the data back to the cpu (host) ([0180]-[0184])." Additionally, the Examiner has argued that Flint teaches the idea of a user being able to disable and enable a virus scanning module (Col. 9, lines 5-24). From this, the Examiner has concluded that the combination of such teachings meet appellant's claimed method "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

Appellant respectfully disagrees. Makita merely teaches two scenarios. First, if a virus is found during the virus check, transmission to the host is stopped ([00183]). Second, if a virus is not found during the virus check, the information is transmitted to the host ([00184]). Clearly, there is no

disclosure of the result when no virus check is performed, since Makita does not allow for this option. Thus, only appellant teaches and claims that "data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module."

In the Examiner's Answer mailed 01/29/2007, the Examiner has argued that "Flint teaches disabling a virus scanner (see column 9 lines 10-15)" and that "when the virus scanner is stopped (i.e. disabled) the session stamp of the file is invalidated (see column 9 lines 3-4)." Additionally, the Examiner has argued that "referring to figure 6, number 611, the session stamp is checked to determine whether it is valid or not," that "when it is not, the file is scanned for viruses and the session stamp is updated," and that "since the virus scanner is stopped at this point the session stamp is updated to state that it is still invalid as described in column 9 lines 3-4." Further, the Examiner has argued that "referring to figure 8, which related to the specifics of when the virus scanner is terminated, the virus scanning program and method is stopped without updating the session stamp to be valid," that "therefore when attempting to access this file the above steps will be repeated as long as the virus scanner is off so the session stamp will never be validated," and that "therefore the file cannot not be accessed as further described with respect to figure 7 and column 10 lines 20-32."

Appellant respectfully disagrees and again notes that the above excerpts relied on by the Examiner merely disclose that "[i]f the user input specifies the termination of the anti-virus program (block 427), a termination process illustrated by block 429 and described in more detail below in conjunction with FIG. 8 is performed" (Col. 9, lines 10-13). Additionally, the excerpts disclose that "[i]f the scanning facility has been stopped, the session stamp of the file is invalidated" (Col. 9, lines 3-4 - emphasis added). Further, with respect to the figures from Flint relied on by the Examiner, Flint discloses "scan[ning] a pre-determined set of the files on the computer (scan set) as a background task," where "[b]eginning with the first file... [i]f the session stamp is found but is invalidated (block 611) by the tests described previously, the file is rescanned at block 607 and the session stamp is updated" (Col. 9, line 63 – Col. 10, line 3 – emphasis added).

Further still, Flint discloses that "when an execution of the method 400 is terminated (FIG. 8), if the user has configured the anti-virus software to save the 'most recently used' (MRU) files for use by the pre-population scan method (block 801), the cache is saved to non-volatile storage at block 803" and that "[t]he current execution of the method is terminated at block 805" (Col. 9, lines 33-39 –

emphasis added). Also, the excerpts disclose that with respect to "acts performed by the computer when a file is accessed," the "on-access scan method 700 first checks for the presence of a session stamp in the directory entry for the file," where "[i]f the session stamp is not found (block 703), the file is scanned for viruses (block 705) and an appropriate session stamp created," and where "[a]n invalid session stamp... causes the corresponding file to be rescanned and the session stamp updated" (Col. 10, lines 20-32 – emphasis added). In addition, Flint discloses that "[i]f the session stamp is valid, it may indicate that the file is infected," where "[t]he user is allowed accesses to the file if uninfected... and denied access if infected" (Col. 10, lines 33-35 – emphasis added).

However, merely disclosing the invalidation of a session stamp of a file if a scanning facility is stopped, in addition to disclosing the accessing of one or more files, where a file is rescanned if the session stamp is invalidated, as in Flint, fails to disclose that "the file cannot... be accessed," as argued by the Examiner, and further fails to teach a technique "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added), as claimed by appellant.

Additionally, saving data to non-volatile storage upon the termination of the scan method, in addition to disclosing that a valid session stamp may indicate that a file is infected, where a user is denied access to the file if it is infected (e.g., has a valid session stamp), and where a session stamp is invalidated upon the stopping of the scanning facility, as in Flint, does not disclose, and in fact *teaches away* from, a technique "wherein a user is allowed to disable the scanning module, and data is precluded from being transmitted from the storage to the central processing unit upon the disabling of the scanning module" (emphasis added), as claimed by appellant.

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be

found in the prior art and not based on appellant's disclosure. *In re Vaeck*,947 F.2d 488, 20 USPQ2d 1438 (Fed.Cir.1991).

Appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above. A notice of allowance or a specific prior art showing of all of appellant's claim limitations, in combination with the remaining claim elements, is respectfully requested.

Group # 2: Claims 35-38

With respect to independent Claim 35, the Examiner has relied on Figure 15 item 413 of Makita to make a prior art showing of appellant's claimed "scanning module coupled to the central processing unit and the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests."

Appellant respectfully asserts that item 413 of Figure 15 is a virus check unit to which "information to be recorded corresponding to the command is supplied" (see [0174] in Makita). Having information supplied to a virus check unit simply does not meet "scanning module adapted for identifying requests from the central processing unit," as claimed by appellant (emphasis added).

Further, the Examiner has relied on Makita's disclosed file management unit (Figure 15 item 211) and the following excerpts from Makita to make a prior art showing of appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning":

> "The file management unit 121 manages the storage of files into, the readout and deletion of files from, and access rights o the recording medium 4 of the external storage 120. The file management unit 121 includes programs for managing the recording medium 4 formatted into a desired logical format in formats corresponding to operation systems such as 12-bit FAT (File Allocation Table) of MS-DOS, the 16-bit FAT of MS-DOS, and UNIX." [0091]

"When a virus is discovered in step S8-5, a transmission to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered (step S8-6)." [0183]

Appellant respectfully asserts that a file management unit that manages files, manages access to files, and manages the formatting of files along with stopping a transmission to the host computer when a virus is discovered as disclosed in Makita (see excerpts above) fails to meet "the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning," as claimed by appellant (emphasis added). Simply nowhere in Makita is there any suggestion of an "event manager module" that is "adapted for receiving results of the scanning" and "adapted to execute an event based on the results of the scanning," as claimed.

In the Advisory Action dated 05/16/2005, the Examiner has relied on paragraph [0174] of Makita in arguing that the CPU in Makita sends a request to the scanning module to scan for data. Thus, the Examiner has concluded that the scanning module must be adapted for identifying the requests from the CPU since it is adapted to receive requests for a data scan.

Appellant respectfully asserts that Makita merely teaches that "[w]hen a command to record information on the recording medium 4 is supplied from the host computer 110 (step S7-1), information to be recorded corresponding to the command is supplied to the virus check engine unit 413" (emphasis added). Thus, the virus check engine in Makita is not adapted for identifying requests, since no request is ever made by the host computer. In particular, the information in Makita is simply supplied to the virus check engine, and a request is not utilized. To emphasize, the host computer in Makita does not send a request to the scanner, but simply sends the information to the scanner. Thus, the scanner in Makita does not have a request to identify or respond to since it is only the information itself which is being sent to the scanner and not a request.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "in Makita the CPU of the host computer sends a command (i.e. request) for access to a file (see paragraph 180), and the file is then accessed and scanned for viruses (see paragraphs 181 and 182)." Additionally, the Examiner has argued that "[t]herefore, the external storage unit (410 of figure 15) contains a system that receives and identifies requests for data, which is also scanned."

Appellant respectfully disagrees, and notes that it appears as though the Examiner is asserting that the external storage 410 of Makita meets appellant's claimed "scanning module." However, appellant respectfully notes that the above excerpts relied on by the Examiner merely disclose that "the host computer 110 supplies a command to read out information from the recording medium 4" and that "information corresponding to the command is read out from the recording medium 4" (Paragraph [0180] – emphasis added). Additionally, the excerpts disclose that "[t]he information read out from the recording medium 4 is supplied to the compression and expansion unit 411," which "expands the information read out from the replaceable recording medium 4" (Paragraph [0181] – emphasis added), and also disclose that "[t]he information expanded in the compression and expansion unit 411 is supplied to the virus check unit 413," where "[t]he virus check unit 413 performs a virus check on the expanded information," where "[i]t is determined whether a virus is discovered in the information read out from the recording medium 4 as a result of the virus check" (Paragraph [0182] – emphasis added). Additionally, Makita teaches that "[a]n external storage 410... includes a compression and expansion unit 411, an optimization unit 412, and a virus check unit 413 in addition to the interface unit 21, the storage unit 22, the nonvolatile memory 212, the file management unit 211, the logical format recognition unit 311, and the logical format execution unit 312" (Paragraph [0168] – emphasis added). Further, Makita teaches that "the storage unit 22 reads out the instructed amount of data from the instructed position [of the recording medium]" (Paragraph [0024] – emphasis added).

However, merely disclosing an external storage system which **includes** a compression and expansion unit, a virus check unit, and a storage unit, where the storage unit reads data from the recording medium, as in Makita, fails to disclose a "scanning module **coupled to**... the storage subsystem controller, the scanning module adapted for identifying the requests from the central processing unit, and scanning the data for malicious code in response to the requests," where the "storage subsystem controller [is] coupled to the storage for controlling access to the data saved therein" (see independent claim 35 – emphasis added), as claimed by appellant.

In addition, in the Advisory Action dated 05/16/2005, the Examiner has relied on the file management unit as described in Makita paragraph [0091], in supporting the present rejection. However, appellant respectfully asserts that such file management unit simply manages "the storage

of files into, the readout and deletion of files from, and access rights to the recording medium 4 of the external storage 120" ([0091]). Thus, the file management unit only manages files with respect to the recording medium.

In Makita, the only mention of scanning such files relates to scanning them when information is read out from the recording medium (see paragraph [0181]). Then, after the scanning, it is determined whether the file is transferred to a host computer (see paragraphs [0182]-[0184]). Since the file management unit only manages files with respect to the recording medium, such file management unit does not manage files with respect to their transmission from the virus check unit to the host computer. Therefore, clearly appellant's claimed "event manager module coupled to the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning" has not been met by the Makita reference.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "as described in paragraphs 183 and 184 the data transmission is either stopped or allowed to continue to the host computer based on the results of virus scanning" and that "[t]herefore a portion of the external storage unit (410) receives the results and another portion causes an event to happen (stopping or allowing transmission to the host) based on those results."

Appellant respectfully disagrees, and notes that it appears as though the Examiner is additionally asserting that the external storage 410 of Makita meets appellant's claimed "event manager module." However, appellant respectfully notes that the above excerpts relied on by the Examiner merely disclose that "[w]hen a virus is discovered... transmission [of data from the recording medium] to the host computer 110 is stopped, and the host computer 110 is notified that the virus is discovered" (Paragraph [0183]), and that "[w]hen no virus is-discovered as a result of the virus check performed by the virus check unit 413, the expanded information is transmitted to the host computer 110" (Paragraph [0183]).

However, merely disclosing that transmission of data from the external storage unit to the host computer is stopped if a virus is discovered by the virus check unit, where the external storage unit **includes** a compression and expansion unit, a virus check unit, and a storage unit, as in Makita, fails

to disclose "an event manager module **coupled to** the scanning module and the central processing unit, the event manager module adapted for receiving results of the scanning from the scanning module, the event manager module adapted to execute an event based on the results of the scanning" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group # 3: Claims 6 and 22

With respect to dependent Claim 6 et al., the Examiner has relied on Makita's paragraph [0213] to meet appellant's claimed technique "wherein the scanning module includes software." Appellant respectfully asserts that paragraph [0213] of Makita simply teaches that the "virus check can be performed even if a virus check program is not installed on the host computer." Thus, the only virus check software program disclosed in Makita relates to a virus checker on the host computer, and not that the scanning module (i.e. virus checker) includes software.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "all virus scanners are a combination of software and hardware for it to run on" and has further argued that "the combined reference of Flint teaches a virus program (i.e. software) and this program is tied to a CPU and disk (see column 1 lines 36-50)."

Appellant respectfully disagrees and notes that the above excerpt from Flint relied on by the Examiner merely discloses that "AV programs scan computer files for known viruses... by comparing each file to a list of 'virus signatures' that are stored in 'virus signature files' or by emulating computer instructions contained within the file to evaluate the effect of the instructions" (Col. 1, lines 36-40). Additionally, the excerpts disclose that "[t]he scanning can be done upon request of a user, when the file is accessed on a mass storage device such as by an application, or on a scheduled basis" and that "[v]irus scanning is, therefore, a resource intensive (CPU and disk I/O) and time-consuming task, especially in the case of access scanning" (Col. 1, lines 40-45).

However, merely disclosing that anti-virus programs scan for viruses by comparing files to virus signatures or by emulating computer instructions, in addition to disclosing that scanning may be done by user request, when a file is accessed by an application, or according to a schedule, and that scanning is time and resource intensive, fails to support the Examiner's assertion that "all virus scanners are a combination of software and hardware for it to run on" (emphasis added), and does not teach a technique "wherein the scanning module includes software" (emphasis added), as specifically claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group # 4: Claims 7 and 23

With respect to dependent Claim 7 et al., the Examiner has relied on Figure 15 of Makita to meet appellant's claimed technique "wherein the scanning module includes hardware." Appellant respectfully asserts that Figure 15 merely shows that the virus check unit 413 is included in the external storage 4 (which may include logic stored on the external storage 4) and not that the virus check unit includes hardware itself.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "all virus scanners are a combination of software and hardware for it to run on" and has further argued that "the combined reference of Flint teaches a virus program (i.e. software) and this program is tied to a CPU and disk (see column 1 lines 36-50)."

Appellant respectfully disagrees and notes that the above excerpt from Flint relied on by the Examiner merely discloses that "AV programs scan computer files for known viruses... by comparing each file to a list of 'virus signatures' that are stored in 'virus signature files' or by emulating computer instructions contained within the file to evaluate the effect of the instructions" (Col. 1, lines 36-40). Additionally, the excerpts disclose that "[t]he scanning can be done upon request of a user, when the file is accessed on a mass storage device such as by an application, or on

a scheduled basis" and that "[v]irus scanning is, therefore, a resource intensive (CPU and disk I/O) and time-consuming task, especially in the case of access scanning" (Col. 1, lines 40-45).

However, merely disclosing that anti-virus programs scan for viruses by comparing files to virus signatures or by emulating computer instructions, in addition to disclosing that scanning may be done by user request, when a file is accessed by an application, or according to a schedule, and that scanning is time and resource intensive, fails to support the Examiner's assertion that "all virus scanners are a combination of software and hardware for it to run on" (emphasis added), and does not teach a technique "wherein the scanning module includes hardware" (emphasis added), as specifically claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group # 5: Claims 12, 13 and 28

With respect to dependent Claim 12 et al., the Examiner has relied on paragraph [0183] of Makita to make a prior art showing of appellant's claimed "disabling the scanning module in response to the event." Appellant respectfully asserts that the above cited reference from Makita merely teaches that "a transmission to the host computer 110 is stopped" ([0183]). Thus, there is simply no disclosure of any sort of "disabling [of] the scanning module" and especially not "in response to the event," as claimed by appellant.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "Makita teaches the disabling of functionality based on an event in paragraph 183 (the stopping of transmission based on the virus scanning results) and Flint teaches disabling a virus scanner based on user input (i.e. an event) (see column 9 lines 10-13)." The Examiner has additionally argued that "[t]herefore the combination teaches disabling the scanning module in response to an event."

Appellant respectfully disagrees and notes that the above excerpts relied on by the Examiner merely disclose that "[w]hen a virus is discovered... a transmission to the host computer 110 is stopped"

(Makita, Paragraph [0183]), and that "[i]f the user input specifies the termination of the anti-virus program... a termination process... is performed" (Flint, Col. 9, lines 10-13 – emphasis added).

However, merely disclosing stopping a transmission to a host computer when a virus is discovered, as in Makita, in addition to performing a termination process based on **user input** specifying the termination of an anti-virus program, as in Flint, does not teach "disabling a virus scanner based on user input (i.e. an event)," as asserted by the Examiner, and fails to disclose "disabling the scanning module in response to the event," where the event is "execut[ed]... based on results of the scanning" (see Claim 10 - emphasis added), in the context claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group # 6: Claims 14 and 30

With respect to dependent Claim 14 et al, the Examiner has relied on Makita's teaching of formatting the recording medium ([0053]-[0054]) to make a prior art showing of appellant's claimed technique "wherein the scanning includes content scanning." The Examiner has stated that content scanning is used to determine a format of the data and to format the data. However, Makita clearly only teaches formatting the recording medium (see specifically paragraph [0054]) and not providing content scanning of the requested data for malicious code, in the manner claimed by appellant.

In the Examiner's Answer mailed 06/23/2008, the Examiner has argued that "the virus check unit scans the requested file to check if the file contains any known viruses (scanning for content)" and that "[t]herefore, Makita teaches content scanning." Appellant respectfully disagrees and notes that the Examiner has failed to provide specific support for the above assertion from the Makita reference.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group # 7: Claim 40

With respect to dependent Claim 40, the Examiner has continued to rely on Flint's disclosed system where "[t]he user or administrator also faces the challenges inherent in maintaining the external database" (Col. 2, lines 19-20) to make a prior art showing of appellant's claimed technique "wherein the user includes a remote administrator."

Appellant respectfully asserts that Flint's basic mention of an administrator that maintains an external database does not meet appellant's "user [that] includes a remote administrator" (Claim 40) in the context of appellant's claim language, such that the "user is allowed to disable the scanning module" (see independent Claim 1).

In the Advisory Action dated 05/16/2005, the Examiner argued that Flint does not provide support for a user being an administrator, but that Flint discloses that a user or administrator can maintain a similar system to that of Makita's and appellant's. The Examiner then concludes by stating that "Flint provides support that a user can be an administrator."

Appellant respectfully asserts that the Examiner's arguments are not clear. First the Examiner states that Flint does not support a user being an administrator, and then the Examiner goes on to state that Flint does provide support that a user can be an administrator. Appellant again argues that the only administrator disclosed in Flint relates to an administrator who maintains a database, and not a remote administrator who can disable the scanning module, as claimed by appellant (see Claim 40 which depends from Claim 1).

In the Examiner's Answer mailed 06/23/2008, the Examiner has stated that "[a]ppellant argues [that] the combined references fail to teach [that] a remote administrator can disable the scanning module" and has further argued that "Flint teaches that a user can disable a virus scanner (see column 9 lines 10-13)." Additionally, the Examiner has argued that "Flint further teaches that [a] user can be an administrator (see column 2 lines 19-20)" and that "[t]herefore, when combined with the remote requests of Makita the combined references teach [that] a remote administrator can disable the scanning module."

Appellant respectfully disagrees and notes that the above excerpts from Flint relied on by the Examiner merely disclose that "[i]f the user input specifies the termination of the anti-virus program... a termination process... is performed" (Col. 9, lines 10-13) and that "[t]he user or administrator also faces the challenges inherent in maintaining the external database" (Col. 2, lines 19-20 – emphasis added).

Appellant respectfully points out that the above excerpts in fact *distinguish* the user from the administrator in disclosing that "[t]he user **or** administrator also faces the challenges inherent in maintaining the external database" (emphasis added). As a result, appellant again argues that the only administrator disclosed in Flint relates to an administrator who maintains a database, and not a remote administrator who can disable the scanning module, as claimed by appellant (see Claim 40 which depends from Claim 1).

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue # 3:

The Examiner has rejected Claim 41 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent Publication No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700, in further view of Browne, U.S. Patent No. 6,272,533.

Group # 1: Claim 41

With respect to dependent Claim 41, the Examiner has relied on Browne to make a prior art showing of appellant's claimed technique "wherein the user is allowed to disable the storage, and the data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage." Specifically, the Examiner has stated that Browne discloses a secure computing system in which a manual switch can be pressed so that data is precluded from being written to a storage device.

Appellant respectfully asserts that Browne merely teaches the "disabling [of the] alteration of data residing on a mass storage device" (see Abstract). Thus, simply disabling the alteration of data, as in Browne, does not meet appellant's specifically claimed "disabling of the storage," let alone disabling the storage such that "data is precluded from being transmitted to the storage from the central processing unit upon the disabling of the storage."

In the Examiner's Answer mailed 06/23/2008, the Examiner has stated that "Browne teaches the use of a read mode that is user activated (see column 4 lines 51-64) and when in read mode data cannot be written to the storage device (see column 8 lines 65-67 'read only')." Additionally, the Examiner has argued that "[t]herefore, Browne discloses [that] a user is allowed to disable the storage, and the data is precluded from being transmitted to the storage upon said disabling." Appellant respectfully disagrees.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue #4:

The Examiner has rejected Claims 42 and 43 under 35 U.S.C. 103(a) as being unpatentable over Makita, U.S. Patent Publication No. 2001/0007120, in view of Flint, U.S. Patent No. 6,735,700, in further view of Browne, U.S. Patent No. 6,272,533.

Group #1: Claim 42

With respect to dependent Claim 42, in the Examiner's Answer mailed 06/23/2008, the Examiner has relied on Col. 9, lines 5-39 from Flint, in addition to Col. 4, lines 61-64 from Browne, to make a prior art showing of appellant's claimed technique "wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled."

Appellant respectfully notes that the above excerpts relied on by the Examiner merely disclose that "when a file is accessed while the anti-virus scanning facility is inactive... the file can also be added to a rescan list in addition to having its session stamp invalidated" and that "when an execution of the method... is terminated... if the user has configured the anti-virus software to save the 'most recently used' (MRU) files for use by the pre-population scan method... the cache is saved to non-volatile storage" (Flint, Col. 9, lines 26-38 – emphasis added). Additionally, the excerpts disclose that "a second manually operative switch selectively disabl[es] the storage device from operating in the write mode of operation" (Browne, Col. 4, lines 62-64 – emphasis added).

However, merely disclosing that a file is accessed while a scanning facility is inactive, in addition to disclosing that a cache is saved when an execution of a scanning method is terminated, as in Flint, in addition to disclosing the disabling of a storage device from operating in a write mode, as in Browne, does not disclose a technique "wherein it is determined whether the storage is disabled only after determining whether the scanning module is disabled" (emphasis added), as claimed by appellant. The prior art excerpts clearly fail to disclose "determin[ing] whether the storage is disabled only after determining whether the scanning module is disabled" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Group #2: Claim 43

With respect to dependent Claim 43, in the Examiner's Answer mailed 06/23/2008, the Examiner has relied on Col. 4, lines 61-64 from Browne to make a prior art showing of appellant's claimed technique "wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit."

Appellant respectfully notes that the above excerpt relied on by the Examiner merely discloses that "a second manually operative switch selectively disabl[es] the storage device from operating in the

write mode of operation" (Browne, Col. 4, lines 62-64 – emphasis added). However, merely disclosing the disabling of a storage device from operating in a write mode, as in Browne, does not disclose a technique "wherein the disabling and enabling of the storage and the scanning module provides increased functionality in conditionally precluding transmission of the data to the storage from the central processing unit" (emphasis added), as claimed by appellant.

Again, appellant respectfully asserts that at least the third element of the *prima facie* case of obviousness has not been met, since the prior art excerpts, as relied upon by the Examiner, fail to teach or suggest all of the claim limitations, as noted above.

Issue #5:

The Examiner has rejected Claims 17, 18, 20-23, 26-32, 34, and 39 under 35 U.S.C. 101 as being directed to non-statutory subject matter.

Group #1: Claims 17, 18, 20-23, and 26-32

In the Examiner's Answer mailed 06/23/2008, the Examiner has stated that "Claims 17, 18, 20-23, 26-32, and 34 relate to a computer program product and claim 39 relates to a system with different means plus function language" and that "[t]he computer program products are merely computer code and the specification allows the means to be merely software." Additionally, the Examiner has argued that "[t]herefore, these claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101." Further, the Examiner has argued that "[t]hey are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter" and that "[a]s such, they fail to fall within a statutory category" and "[t]hey are, at best, functional descriptive material per se."

Appellant respectfully disagrees. Clearly, any [new and useful] process, machine, manufacture or composition of matter under the sun that is made by man is the proper subject matter of a patent. *Alappat*, 33 F.3d at 1542, 31 USPQ2d at 1556; *Warmerdam*, 33 F.3d at 1358, 31 USPQ2d at 1757 (Fed. Cir. 1994) In the present case, a "computer program product for scanning data read from storage" (see Claim 17) is clearly an example of an article of manufacture.

The subject matter that courts have found to be outside of, or exceptions to, such four statutory categories of invention is limited to abstract ideas, laws of nature and natural phenomena. In the present case, the claims at issue clearly do not fall into such categories. Further, even if the Examiner were to attempt to argue that the claims at issue did allegedly fall into such categories, appellant asserts that the claims are clearly directed to a practical application thereof.

Per MPEP 2106, "[a] claimed invention is directed to a practical application of a 35 U.S.C. 101 judicial exception when it:

> (A) 'transforms' an article or physical object to a different state or thing; or
> (B) otherwise produces a useful, concrete and tangible result."

In the present case, appellant teaches and claims "computer code for **transmitting** the data from the storage to the central processing unit" (see Claim 17 – emphasis added). By virtue of the claimed "transmitting," appellant clearly teaches and claims a "transformation" of an article or physical object to a different state or thing. Further, appellant claims "computer code for **scanning the requested data** for malicious code" (see Claim 17 – emphasis added). Such specifically claimed substantial limitations clearly constitute a useful feature that provides tangible real-world results which can be substantially repeatable or substantially produce the same result again.

For these and various other reasons, appellant respectfully contends that the aforementioned independent claim at issue clearly meets the requirements of 35 U.S.C. 101. Additionally, the remaining dependent claims at issue clearly meet the requirements of 35 U.S.C. 101, in view of their dependence on such independent claims.

Group #2: Claim 34

In the Examiner's Answer mailed 06/23/2008, the Examiner has stated that "Claims 17, 18, 20-23, 26-32, and 34 relate to a computer program product and claim 39 relates to a system with different means plus function language" and that "[t]he computer program products are merely computer code and the specification allows the means to be merely software." Additionally, the Examiner has argued that "[t]herefore, these claims lack the necessary physical articles or objects to constitute a

machine or a manufacture within the meaning of 35 USC 101." Further, the Examiner has argued that "[t]hey are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter" and that "[a]s such, they fail to fall within a statutory category" and "[t]hey are, at best, functional descriptive material per se."

Appellant respectfully disagrees. Clearly, any [new and useful] process, machine, manufacture or composition of matter under the sun that is made by man is the proper subject matter of a patent. *Alappat*, 33 F.3d at 1542, 31 USPQ2d at 1556; *Warmerdam*, 33 F.3d at 1358, 31 USPQ2d at 1757 (Fed. Cir. 1994) In the present case, a "computer program product for scanning data written to storage" (see Claim 34) is clearly an example of an article of manufacture.

The subject matter that courts have found to be outside of, or exceptions to, such four statutory categories of invention is limited to abstract ideas, laws of nature and natural phenomena. In the present case, the claims at issue clearly do not fall into such categories. Further, even if the Examiner were to attempt to argue that the claims at issue did allegedly fall into such categories, appellant asserts that the claims are clearly directed to a practical application thereof.

Per MPEP 2106, "[a] claimed invention is directed to a practical application of a 35 U.S.C. 101 judicial exception when it:

> (A) 'transforms' an article or physical object to a different state or thing; or
> (B) otherwise produces a useful, concrete and tangible result."

In the present case, appellant teaches and claims "computer code for **writing** the data to the storage" (see Claim 34 – emphasis added). By virtue of the claimed "writing," appellant clearly teaches and claims a "transformation" of an article or physical object to a different state or thing. Further, appellant claims "computer code for **scanning the data** for malicious code" (see Claim 34 – emphasis added). Such specifically claimed substantial limitations clearly constitute a useful feature that provides tangible real-world results which can be substantially repeatable or substantially produce the same result again.

For these and various other reasons, appellant respectfully contends that the aforementioned independent claim at issue clearly meets the requirements of 35 U.S.C. 101.

Group #3: Claim 39

In the Examiner's Answer mailed 06/23/2008, the Examiner has stated that "Claims 17, 18, 20-23, 26-32, and 34 relate to a computer program product and claim 39 relates to a system with different means plus function language" and that "[t]he computer program products are merely computer code and the specification allows the means to be merely software." Additionally, the Examiner has argued that "[t]herefore, these claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101." Further, the Examiner has argued that "[t]hey are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter" and that "[a]s such, they fail to fall within a statutory category" and "[t]hey are, at best, functional descriptive material per se."

Appellant respectfully disagrees. Clearly, any [new and useful] process, machine, manufacture or composition of matter under the sun that is made by man is the proper subject matter of a patent. *Alappat*, 33 F.3d at 1542, 31 USPQ2d at 1556; *Warmerdam*, 33 F.3d at 1358, 31 USPQ2d at 1757 (Fed. Cir. 1994)

The subject matter that courts have found to be outside of, or exceptions to, such four statutory categories of invention is limited to abstract ideas, laws of nature and natural phenomena. In the present case, the claims at issue clearly do not fall into such categories. Further, even if the Examiner were to attempt to argue that the claims at issue did allegedly fall into such categories, appellant asserts that the claims are clearly directed to a practical application thereof.

Per MPEP 2106, "[a] claimed invention is directed to a practical application of a 35 U.S.C. 101 judicial exception when it:

(A) 'transforms' an article or physical object to a different state or thing; or
(B) otherwise produces a useful, concrete and tangible result."

In the present case, appellant teaches and claims "means for **saving** data therein" (see Claim 39 – emphasis added). By virtue of the claimed "saving," appellant clearly teaches and claims a "transformation" of an article or physical object to a different state or thing. Further, appellant

claims "means for **controlling access to the data** saved therein" as well as "means for **issuing read requests** for reading the data saved therein for processing purposes" and "means for... **scanning the data for malicious code** in response to the requests" (see Claim 39 – emphasis added). Such specifically claimed substantial limitations clearly constitute a useful feature that provides tangible real-world results which can be substantially repeatable or substantially produce the same result again.

For these and various other reasons, appellant respectfully contends that the aforementioned independent claim at issue clearly meets the requirements of 35 U.S.C. 101.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P020).

Respectfully submitted,

By: /KEVINZILKA/ Date: August 21, 2008
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660